Scan Report

June 25, 2025

Summary

This document reports on the results of an automatic security scan. All dates are displayed using the timezone "Coordinated Universal Time", which is abbreviated "UTC". The task was "intense scan". The scan started at Wed Jun 25 03:07:39 2025 UTC and ended at Wed Jun 25 22:31:30 2025 UTC. The report first summarises the results found. Then, for each host, the report describes every issue found. Please consider the advice given in each description, in order to rectify the issue.

Contents

1 Result Overview

Host	High	Medium	Low	Log	False Positive
192.168.1.104	1	4	1	0	0
127.0.0.1 localhost	0	2	0	0	0
192.168.1.10	0	3	3	0	0
Total: 3	1	9	4	0	0

Vendor security updates are not trusted.
Overrides are off. Even when a result has an override, this report uses the actual threat of the result.
Information on overrides is included in the report.
Notes are included in the report.
This report might not show details of all issues that were found.
Issues with the threat level “Log” are not shown.
Issues with the threat level “Debug” are not shown.
Issues with the threat level “False Positive” are not shown.
Only results with a minimum QoD of 70 are shown.

This report contains all 14 results selected by the filtering described above. Before filtering there were 186 results.

2 Results per Host

2.1 192.168.1.104

Host scan start	Wed Jun 25 03:08:12 2025 UTC
Host scan end	Wed Jun 25 22:31:22 2025 UTC

Service (Port)	Threat Level
1515/tcp	High
443/tcp	Medium
55000/tcp	Medium
1515/tcp	Medium
22/tcp	Low

2.1.1 High 1515/tcp

High (CVSS: 7.5)

NVT: Unprotected OSSEC/Wazuh ossec-authd (authd Protocol)

. . . continues on next page . . .

. . . continued from previous page . . .

Product detection result

```
cpe:/a:ossec:authd
Detected by OSSEC/Wazuh ossec-authd Service Detection (TCP) (OID: 1.3.6.1.4.1.25
↪623.1.0.108546)
```

Summary

The remote OSSEC/Wazuh ossec-authd service is not protected by password authentication or client certificate verification.

Quality of Detection (QoD): 99%

Vulnerability Detection Result

Vulnerability was detected according to the Vulnerability Detection Method.

Impact

This issue may be misused by a remote attacker to register arbitrary agents at the remote service or overwrite the registration of existing ones taking them out of service.

Solution:

Solution type: Workaround

Enable password authentication or client certificate verification within the configuration of ossec-authd. Please see the manual of this service for more information.

Vulnerability Insight

It was possible to connect to the remote OSSEC/Wazuh ossec-authd service without providing a password or a valid client certificate.

Vulnerability Detection Method

Evaluate if the remote OSSEC/Wazuh ossec-authd service is protected by password authentication or client certificate verification.
Note:
If the scanned network is e.g. a private LAN which contains systems not accessible to the public (access restricted) and it is accepted that the target host is accessible without authentication please set the 'Network type' configuration of the following VT to 'Private LAN':
Global variable settings (OID: 1.3.6.1.4.1.25623.1.0.12288)
Details: `Unprotected OSSEC/Wazuh ossec-authd (authd Protocol)`
OID:1.3.6.1.4.1.25623.1.0.108547
Version used: `2025-04-29T05:39:55Z`

Product Detection Result

Product: `cpe:/a:ossec:authd`
Method: `OSSEC/Wazuh ossec-authd Service Detection (TCP)`
OID: 1.3.6.1.4.1.25623.1.0.108546)

[return to 192.168.1.104]

2.1.2 Medium 443/tcp

Medium (CVSS: 5.8)

NVT: SSL/TLS: Renegotiation MITM Vulnerability (CVE-2009-3555)

Summary

The remote SSL/TLS service is prone to a man-in-the-middle (MITM) vulnerability.

Quality of Detection (QoD): 70%

Vulnerability Detection Result

```
Protocol Version | Successful re-done SSL/TLS handshakes (Renegotiation) over an
↪ existing / already established SSL/TLS connection
--------------------------------------------------------------------------------
↪------------------------------------------------
TLSv1.2          | 2
```

Impact

A remote, unauthenticated attacker may be able to inject an arbitrary amount of chosen plaintext into the beginning of the application protocol stream. This could allow and attacker to issue HTTP requests, or take action impersonating the user, among other consequences.

Solution:

Solution type: VendorFix

Users should contact their vendors for specific patch information.

General solution options are:

- remove/disable renegotiation capabilities altogether from/in the affected SSL/TLS service
- enable Safe/Secure renegotiation (RFC5746) for the affected SSL/TLS service

Affected Software/OS

The TLS protocol, and the SSL protocol 3.0 and possibly earlier, as used in Microsoft Internet Information Services (IIS) 7.0, mod_ssl in the Apache HTTP Server 2.2.14 and earlier, OpenSSL before 0.9.8l, GnuTLS 2.8.5 and earlier, Mozilla Network Security Services (NSS) 3.12.4 and earlier, multiple Cisco products, and other products.

Vulnerability Insight

The flaw exists because the remote SSL/TLS service does not properly associate renegotiation handshakes with an existing connection, which allows MITM attackers to insert data into HTTPS sessions, and possibly other types of sessions protected by TLS or SSL, by sending an unauthenticated request that is processed retroactively by a server in a post-renegotiation context, related to a 'plaintext injection' attack, aka the 'Project Mogul' issue.

Vulnerability Detection Method

Checks if the remote service allows to re-do the same SSL/TLS handshake (Renegotiation) over an existing / already established SSL/TLS connection.

. . . continues on next page . . .

... continued from previous page ...

Details: SSL/TLS: Renegotiation MITM Vulnerability (CVE-2009-3555)

OID:1.3.6.1.4.1.25623.1.0.117758

Version used: 2024-09-27T05:05:23Z

References

```
cve: CVE-2009-3555
url: https://blog.g-sec.lu/2009/11/tls-sslv3-renegotiation-vulnerability.html
url: https://www.g-sec.lu/practicaltls.pdf
url: https://www.kb.cert.org/vuls/id/120541
url: https://orchilles.com/ssl-renegotiation-dos/
url: https://lwn.net/Articles/362234/
url: https://kb.fortinet.com/kb/documentLink.do?externalID=FD36385
url: https://datatracker.ietf.org/doc/html/rfc5746
url: https://mailarchive.ietf.org/arch/msg/tls/Y1O3HUcq9T94rMLCGPTTozURtSI/
cert-bund: CB-K17/1878
cert-bund: CB-K17/1642
cert-bund: CB-K15/0637
dfn-cert: DFN-CERT-2017-1960
dfn-cert: DFN-CERT-2017-1722
dfn-cert: DFN-CERT-2015-0664
dfn-cert: DFN-CERT-2013-0321
dfn-cert: DFN-CERT-2012-1377
dfn-cert: DFN-CERT-2012-0828
dfn-cert: DFN-CERT-2012-0613
dfn-cert: DFN-CERT-2011-1720
dfn-cert: DFN-CERT-2011-1138
dfn-cert: DFN-CERT-2011-1137
dfn-cert: DFN-CERT-2011-0712
dfn-cert: DFN-CERT-2011-0700
dfn-cert: DFN-CERT-2011-0321
dfn-cert: DFN-CERT-2011-0193
dfn-cert: DFN-CERT-2011-0185
dfn-cert: DFN-CERT-2011-0181
dfn-cert: DFN-CERT-2011-0116
dfn-cert: DFN-CERT-2011-0021
dfn-cert: DFN-CERT-2011-0020
dfn-cert: DFN-CERT-2011-0019
dfn-cert: DFN-CERT-2010-1762
dfn-cert: DFN-CERT-2010-1731
dfn-cert: DFN-CERT-2010-1710
dfn-cert: DFN-CERT-2010-1702
dfn-cert: DFN-CERT-2010-1650
dfn-cert: DFN-CERT-2010-1647
dfn-cert: DFN-CERT-2010-1527
dfn-cert: DFN-CERT-2010-1500
dfn-cert: DFN-CERT-2010-1439
dfn-cert: DFN-CERT-2010-1424
```

... continues on next page ...

. . . continued from previous page . . .

```
dfn-cert: DFN-CERT-2010-1406
dfn-cert: DFN-CERT-2010-1405
dfn-cert: DFN-CERT-2010-1387
dfn-cert: DFN-CERT-2010-1385
dfn-cert: DFN-CERT-2010-1380
dfn-cert: DFN-CERT-2010-1368
dfn-cert: DFN-CERT-2010-1293
dfn-cert: DFN-CERT-2010-1227
dfn-cert: DFN-CERT-2010-1052
dfn-cert: DFN-CERT-2010-1009
dfn-cert: DFN-CERT-2010-1000
dfn-cert: DFN-CERT-2010-0899
dfn-cert: DFN-CERT-2010-0859
dfn-cert: DFN-CERT-2010-0833
dfn-cert: DFN-CERT-2010-0815
dfn-cert: DFN-CERT-2010-0775
dfn-cert: DFN-CERT-2010-0729
dfn-cert: DFN-CERT-2010-0725
dfn-cert: DFN-CERT-2010-0707
dfn-cert: DFN-CERT-2010-0705
dfn-cert: DFN-CERT-2010-0669
dfn-cert: DFN-CERT-2010-0639
dfn-cert: DFN-CERT-2010-0619
dfn-cert: DFN-CERT-2010-0618
dfn-cert: DFN-CERT-2010-0603
dfn-cert: DFN-CERT-2010-0586
dfn-cert: DFN-CERT-2010-0579
dfn-cert: DFN-CERT-2010-0562
dfn-cert: DFN-CERT-2010-0558
dfn-cert: DFN-CERT-2010-0544
dfn-cert: DFN-CERT-2010-0539
dfn-cert: DFN-CERT-2010-0525
dfn-cert: DFN-CERT-2010-0504
dfn-cert: DFN-CERT-2010-0498
dfn-cert: DFN-CERT-2010-0491
dfn-cert: DFN-CERT-2010-0488
dfn-cert: DFN-CERT-2010-0485
dfn-cert: DFN-CERT-2010-0456
dfn-cert: DFN-CERT-2010-0455
dfn-cert: DFN-CERT-2010-0451
dfn-cert: DFN-CERT-2010-0413
dfn-cert: DFN-CERT-2010-0411
dfn-cert: DFN-CERT-2010-0410
dfn-cert: DFN-CERT-2010-0407
dfn-cert: DFN-CERT-2010-0406
dfn-cert: DFN-CERT-2010-0405
dfn-cert: DFN-CERT-2010-0388
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
dfn-cert: DFN-CERT-2010-0370
dfn-cert: DFN-CERT-2010-0339
dfn-cert: DFN-CERT-2010-0303
dfn-cert: DFN-CERT-2010-0273
dfn-cert: DFN-CERT-2010-0201
dfn-cert: DFN-CERT-2010-0166
dfn-cert: DFN-CERT-2010-0050
dfn-cert: DFN-CERT-2010-0030
dfn-cert: DFN-CERT-2009-1833
dfn-cert: DFN-CERT-2009-1821
dfn-cert: DFN-CERT-2009-1820
dfn-cert: DFN-CERT-2009-1809
dfn-cert: DFN-CERT-2009-1805
dfn-cert: DFN-CERT-2009-1757
dfn-cert: DFN-CERT-2009-1755
dfn-cert: DFN-CERT-2009-1725
dfn-cert: DFN-CERT-2009-1719
dfn-cert: DFN-CERT-2009-1689
dfn-cert: DFN-CERT-2009-1688
dfn-cert: DFN-CERT-2009-1654
dfn-cert: DFN-CERT-2009-1653
dfn-cert: DFN-CERT-2009-1646
dfn-cert: DFN-CERT-2009-1643
dfn-cert: DFN-CERT-2009-1630
dfn-cert: DFN-CERT-2009-1623
dfn-cert: DFN-CERT-2009-1603
dfn-cert: DFN-CERT-2009-1602
dfn-cert: DFN-CERT-2009-1584
dfn-cert: DFN-CERT-2009-1578
```

[return to 192.168.1.104]

2.1.3 Medium 55000/tcp

Medium (CVSS: 5.8)

NVT: SSL/TLS: Renegotiation MITM Vulnerability (CVE-2009-3555)

Summary
The remote SSL/TLS service is prone to a man-in-the-middle (MITM) vulnerability.

Quality of Detection (QoD): 70%

Vulnerability Detection Result

```
Protocol Version | Successful re-done SSL/TLS handshakes (Renegotiation) over an
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
↪ existing / already established SSL/TLS connection
---------------------------------------------------------------------------------
↪---------------------------------------------------
TLSv1.2           | 2
```

Impact

A remote, unauthenticated attacker may be able to inject an arbitrary amount of chosen plaintext into the beginning of the application protocol stream. This could allow and attacker to issue HTTP requests, or take action impersonating the user, among other consequences.

Solution:

Solution type: VendorFix

Users should contact their vendors for specific patch information.

General solution options are:

- remove/disable renegotiation capabilities altogether from/in the affected SSL/TLS service
- enable Safe/Secure renegotiation (RFC5746) for the affected SSL/TLS service

Affected Software/OS

The TLS protocol, and the SSL protocol 3.0 and possibly earlier, as used in Microsoft Internet Information Services (IIS) 7.0, mod_ssl in the Apache HTTP Server 2.2.14 and earlier, OpenSSL before 0.9.8l, GnuTLS 2.8.5 and earlier, Mozilla Network Security Services (NSS) 3.12.4 and earlier, multiple Cisco products, and other products.

Vulnerability Insight

The flaw exists because the remote SSL/TLS service does not properly associate renegotiation handshakes with an existing connection, which allows MITM attackers to insert data into HTTPS sessions, and possibly other types of sessions protected by TLS or SSL, by sending an unauthenticated request that is processed retroactively by a server in a post-renegotiation context, related to a 'plaintext injection' attack, aka the 'Project Mogul' issue.

Vulnerability Detection Method

Checks if the remote service allows to re-do the same SSL/TLS handshake (Renegotiation) over an existing / already established SSL/TLS connection.

Details: `SSL/TLS: Renegotiation MITM Vulnerability (CVE-2009-3555)`

OID:1.3.6.1.4.1.25623.1.0.117758

Version used: `2024-09-27T05:05:23Z`

References

```
cve: CVE-2009-3555
url: https://blog.g-sec.lu/2009/11/tls-sslv3-renegotiation-vulnerability.html
url: https://www.g-sec.lu/practicaltls.pdf
url: https://www.kb.cert.org/vuls/id/120541
url: https://orchilles.com/ssl-renegotiation-dos/
url: https://lwn.net/Articles/362234/
url: https://kb.fortinet.com/kb/documentLink.do?externalID=FD36385
url: https://datatracker.ietf.org/doc/html/rfc5746
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
url: https://mailarchive.ietf.org/arch/msg/tls/Y1O3HUcq9T94rMLCGPTTozURtSI/
cert-bund: CB-K17/1878
cert-bund: CB-K17/1642
cert-bund: CB-K15/0637
dfn-cert: DFN-CERT-2017-1960
dfn-cert: DFN-CERT-2017-1722
dfn-cert: DFN-CERT-2015-0664
dfn-cert: DFN-CERT-2013-0321
dfn-cert: DFN-CERT-2012-1377
dfn-cert: DFN-CERT-2012-0828
dfn-cert: DFN-CERT-2012-0613
dfn-cert: DFN-CERT-2011-1720
dfn-cert: DFN-CERT-2011-1138
dfn-cert: DFN-CERT-2011-1137
dfn-cert: DFN-CERT-2011-0712
dfn-cert: DFN-CERT-2011-0700
dfn-cert: DFN-CERT-2011-0321
dfn-cert: DFN-CERT-2011-0193
dfn-cert: DFN-CERT-2011-0185
dfn-cert: DFN-CERT-2011-0181
dfn-cert: DFN-CERT-2011-0116
dfn-cert: DFN-CERT-2011-0021
dfn-cert: DFN-CERT-2011-0020
dfn-cert: DFN-CERT-2011-0019
dfn-cert: DFN-CERT-2010-1762
dfn-cert: DFN-CERT-2010-1731
dfn-cert: DFN-CERT-2010-1710
dfn-cert: DFN-CERT-2010-1702
dfn-cert: DFN-CERT-2010-1650
dfn-cert: DFN-CERT-2010-1647
dfn-cert: DFN-CERT-2010-1527
dfn-cert: DFN-CERT-2010-1500
dfn-cert: DFN-CERT-2010-1439
dfn-cert: DFN-CERT-2010-1424
dfn-cert: DFN-CERT-2010-1406
dfn-cert: DFN-CERT-2010-1405
dfn-cert: DFN-CERT-2010-1387
dfn-cert: DFN-CERT-2010-1385
dfn-cert: DFN-CERT-2010-1380
dfn-cert: DFN-CERT-2010-1368
dfn-cert: DFN-CERT-2010-1293
dfn-cert: DFN-CERT-2010-1227
dfn-cert: DFN-CERT-2010-1052
dfn-cert: DFN-CERT-2010-1009
dfn-cert: DFN-CERT-2010-1000
dfn-cert: DFN-CERT-2010-0899
dfn-cert: DFN-CERT-2010-0859
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
dfn-cert: DFN-CERT-2010-0833
dfn-cert: DFN-CERT-2010-0815
dfn-cert: DFN-CERT-2010-0775
dfn-cert: DFN-CERT-2010-0729
dfn-cert: DFN-CERT-2010-0725
dfn-cert: DFN-CERT-2010-0707
dfn-cert: DFN-CERT-2010-0705
dfn-cert: DFN-CERT-2010-0669
dfn-cert: DFN-CERT-2010-0639
dfn-cert: DFN-CERT-2010-0619
dfn-cert: DFN-CERT-2010-0618
dfn-cert: DFN-CERT-2010-0603
dfn-cert: DFN-CERT-2010-0586
dfn-cert: DFN-CERT-2010-0579
dfn-cert: DFN-CERT-2010-0562
dfn-cert: DFN-CERT-2010-0558
dfn-cert: DFN-CERT-2010-0544
dfn-cert: DFN-CERT-2010-0539
dfn-cert: DFN-CERT-2010-0525
dfn-cert: DFN-CERT-2010-0504
dfn-cert: DFN-CERT-2010-0498
dfn-cert: DFN-CERT-2010-0491
dfn-cert: DFN-CERT-2010-0488
dfn-cert: DFN-CERT-2010-0485
dfn-cert: DFN-CERT-2010-0456
dfn-cert: DFN-CERT-2010-0455
dfn-cert: DFN-CERT-2010-0451
dfn-cert: DFN-CERT-2010-0413
dfn-cert: DFN-CERT-2010-0411
dfn-cert: DFN-CERT-2010-0410
dfn-cert: DFN-CERT-2010-0407
dfn-cert: DFN-CERT-2010-0406
dfn-cert: DFN-CERT-2010-0405
dfn-cert: DFN-CERT-2010-0388
dfn-cert: DFN-CERT-2010-0370
dfn-cert: DFN-CERT-2010-0339
dfn-cert: DFN-CERT-2010-0303
dfn-cert: DFN-CERT-2010-0273
dfn-cert: DFN-CERT-2010-0201
dfn-cert: DFN-CERT-2010-0166
dfn-cert: DFN-CERT-2010-0050
dfn-cert: DFN-CERT-2010-0030
dfn-cert: DFN-CERT-2009-1833
dfn-cert: DFN-CERT-2009-1821
dfn-cert: DFN-CERT-2009-1820
dfn-cert: DFN-CERT-2009-1809
dfn-cert: DFN-CERT-2009-1805
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
dfn-cert: DFN-CERT-2009-1757
dfn-cert: DFN-CERT-2009-1755
dfn-cert: DFN-CERT-2009-1725
dfn-cert: DFN-CERT-2009-1719
dfn-cert: DFN-CERT-2009-1689
dfn-cert: DFN-CERT-2009-1688
dfn-cert: DFN-CERT-2009-1654
dfn-cert: DFN-CERT-2009-1653
dfn-cert: DFN-CERT-2009-1646
dfn-cert: DFN-CERT-2009-1643
dfn-cert: DFN-CERT-2009-1630
dfn-cert: DFN-CERT-2009-1623
dfn-cert: DFN-CERT-2009-1603
dfn-cert: DFN-CERT-2009-1602
dfn-cert: DFN-CERT-2009-1584
dfn-cert: DFN-CERT-2009-1578
```

Medium (CVSS: 5.0)

NVT: SSL/TLS: Renegotiation DoS Vulnerability (CVE-2011-1473, CVE-2011-5094)

Summary

The remote SSL/TLS service is prone to a denial of service (DoS) vulnerability.

Quality of Detection (QoD): 70%

Vulnerability Detection Result

```
The following indicates that the remote SSL/TLS service is affected:
Protocol Version | Successful re-done SSL/TLS handshakes (Renegotiation) over an
↪ existing / already established SSL/TLS connection
--------------------------------------------------------------------------------
↪---------------------------------------------------
TLSv1.2          | 10
```

Impact

The flaw might make it easier for remote attackers to cause a DoS (CPU consumption) by performing many renegotiations within a single connection.

Solution:

Solution type: VendorFix

Users should contact their vendors for specific patch information.

A general solution is to remove/disable renegotiation capabilities altogether from/in the affected SSL/TLS service.

Affected Software/OS

. . . continues on next page . . .

. . . continued from previous page . . .

Every SSL/TLS service which does not properly restrict client-initiated renegotiation.

Vulnerability Insight

The flaw exists because the remote SSL/TLS service does not properly restrict client-initiated renegotiation within the SSL and TLS protocols.

Note: The referenced CVEs are affecting OpenSSL and Mozilla Network Security Services (NSS) but both are in a DISPUTED state with the following rationale:

> It can also be argued that it is the responsibility of server deployments, not a security library, to prevent or limit renegotiation when it is inappropriate within a specific environment.

Both CVEs are still kept in this VT as a reference to the origin of this flaw.

Vulnerability Detection Method

Checks if the remote service allows to re-do the same SSL/TLS handshake (Renegotiation) over an existing / already established SSL/TLS connection.

Details: `SSL/TLS: Renegotiation DoS Vulnerability (CVE-2011-1473, CVE-2011-5094)`

OID:1.3.6.1.4.1.25623.1.0.117761

Version used: `2024-09-27T05:05:23Z`

References

cve: CVE-2011-1473
cve: CVE-2011-5094
url: https://web.archive.org/web/20211201133213/https://orchilles.com/ssl-renego
↪tiation-dos/
url: https://mailarchive.ietf.org/arch/msg/tls/wdg46VE_jkYBbgJ5yE4P9nQ-8IU/
url: https://vincent.bernat.ch/en/blog/2011-ssl-dos-mitigation
url: https://www.openwall.com/lists/oss-security/2011/07/08/2
cert-bund: WID-SEC-2024-1591
cert-bund: WID-SEC-2024-0796
cert-bund: WID-SEC-2023-1435
cert-bund: CB-K17/0980
cert-bund: CB-K17/0979
cert-bund: CB-K14/0772
cert-bund: CB-K13/0915
cert-bund: CB-K13/0462
dfn-cert: DFN-CERT-2025-0933
dfn-cert: DFN-CERT-2017-1013
dfn-cert: DFN-CERT-2017-1012
dfn-cert: DFN-CERT-2014-0809
dfn-cert: DFN-CERT-2013-1928
dfn-cert: DFN-CERT-2012-1112

[return to 192.168.1.104]

2.1.4 Medium 1515/tcp

Medium (CVSS: 5.0)

NVT: SSL/TLS: Renegotiation DoS Vulnerability (CVE-2011-1473, CVE-2011-5094)

Summary

The remote SSL/TLS service is prone to a denial of service (DoS) vulnerability.

Quality of Detection (QoD): 70%

Vulnerability Detection Result

```
The following indicates that the remote SSL/TLS service is affected:
Protocol Version | Successful re-done SSL/TLS handshakes (Renegotiation) over an
↪ existing / already established SSL/TLS connection
--------------------------------------------------------------------------------
↪---------------------------------------------------
TLSv1.2          | 10
```

Impact

The flaw might make it easier for remote attackers to cause a DoS (CPU consumption) by performing many renegotiations within a single connection.

Solution:

Solution type: VendorFix

Users should contact their vendors for specific patch information.

A general solution is to remove/disable renegotiation capabilities altogether from/in the affected SSL/TLS service.

Affected Software/OS

Every SSL/TLS service which does not properly restrict client-initiated renegotiation.

Vulnerability Insight

The flaw exists because the remote SSL/TLS service does not properly restrict client-initiated renegotiation within the SSL and TLS protocols.

Note: The referenced CVEs are affecting OpenSSL and Mozilla Network Security Services (NSS) but both are in a DISPUTED state with the following rationale:

> It can also be argued that it is the responsibility of server deployments, not a security library, to prevent or limit renegotiation when it is inappropriate within a specific environment.

Both CVEs are still kept in this VT as a reference to the origin of this flaw.

Vulnerability Detection Method

Checks if the remote service allows to re-do the same SSL/TLS handshake (Renegotiation) over an existing / already established SSL/TLS connection.

Details: `SSL/TLS: Renegotiation DoS Vulnerability (CVE-2011-1473, CVE-2011-5094)`

OID:1.3.6.1.4.1.25623.1.0.117761

Version used: `2024-09-27T05:05:23Z`

. . . continues on next page . . .

. . . continued from previous page . . .

References

```
cve: CVE-2011-1473
cve: CVE-2011-5094
url: https://web.archive.org/web/20211201133213/https://orchilles.com/ssl-renego
↪tiation-dos/
url: https://mailarchive.ietf.org/arch/msg/tls/wdg46VE_jkYBbgJ5yE4P9nQ-8IU/
url: https://vincent.bernat.ch/en/blog/2011-ssl-dos-mitigation
url: https://www.openwall.com/lists/oss-security/2011/07/08/2
cert-bund: WID-SEC-2024-1591
cert-bund: WID-SEC-2024-0796
cert-bund: WID-SEC-2023-1435
cert-bund: CB-K17/0980
cert-bund: CB-K17/0979
cert-bund: CB-K14/0772
cert-bund: CB-K13/0915
cert-bund: CB-K13/0462
dfn-cert: DFN-CERT-2025-0933
dfn-cert: DFN-CERT-2017-1013
dfn-cert: DFN-CERT-2017-1012
dfn-cert: DFN-CERT-2014-0809
dfn-cert: DFN-CERT-2013-1928
dfn-cert: DFN-CERT-2012-1112
```

[return to 192.168.1.104]

2.1.5 Low 22/tcp

Low (CVSS: 2.6)

NVT: Weak MAC Algorithm(s) Supported (SSH)

Product detection result

```
cpe:/a:ietf:secure_shell_protocol
Detected by SSH Protocol Algorithms Supported (OID: 1.3.6.1.4.1.25623.1.0.105565
↪)
```

Summary

The remote SSH server is configured to allow / support weak MAC algorithm(s).

Quality of Detection (QoD): 80%

Vulnerability Detection Result

```
The remote SSH server supports the following weak client-to-server MAC algorithm
↪(s):
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
umac-64-etm@openssh.com
umac-64@openssh.com
The remote SSH server supports the following weak server-to-client MAC algorithm
↪(s):
umac-64-etm@openssh.com
umac-64@openssh.com
```

Solution:
Solution type: Mitigation
Disable the reported weak MAC algorithm(s).

Vulnerability Detection Method
Checks the supported MAC algorithms (client-to-server and server-to-client) of the remote SSH server.
Currently weak MAC algorithms are defined as the following:
- MD5 based algorithms
- 96-bit based algorithms
- 64-bit based algorithms
- 'none' algorithm

Details: `Weak MAC Algorithm(s) Supported (SSH)`
OID:1.3.6.1.4.1.25623.1.0.105610
Version used: `2024-06-14T05:05:48Z`

Product Detection Result
Product: `cpe:/a:ietf:secure_shell_protocol`
Method: `SSH Protocol Algorithms Supported`
OID: 1.3.6.1.4.1.25623.1.0.105565)

References
```
url: https://www.rfc-editor.org/rfc/rfc6668
url: https://www.rfc-editor.org/rfc/rfc4253#section-6.4
```

[return to 192.168.1.104]

2.2 127.0.0.1

Host scan start	Wed Jun 25 03:08:12 2025 UTC
Host scan end	Wed Jun 25 22:20:44 2025 UTC

Service (Port)	Threat Level
5432/tcp	Medium
9392/tcp	Medium

2.2.1 Medium 5432/tcp

Medium (CVSS: 5.9)

NVT: SSL/TLS: Report Weak Cipher Suites

Product detection result

```
cpe:/a:ietf:transport_layer_security
Detected by SSL/TLS: Report Supported Cipher Suites (OID: 1.3.6.1.4.1.25623.1.0.
↪802067)
```

Summary

This routine reports all weak SSL/TLS cipher suites accepted by a service.

Quality of Detection (QoD): 98%

Vulnerability Detection Result

```
'Weak' cipher suites accepted by this service via the TLSv1.2 protocol:
TLS_RSA_WITH_SEED_CBC_SHA
```

Impact

This could allow remote attackers to obtain sensitive information or have other, unspecified impacts.

Solution:

Solution type: Mitigation

The configuration of this services should be changed so that it does not accept the listed weak cipher suites anymore.

Please see the references for more resources supporting you with this task.

Affected Software/OS

All services providing an encrypted communication using weak SSL/TLS cipher suites.

Vulnerability Insight

These rules are applied for the evaluation of the cryptographic strength:

- RC4 is considered to be weak (CVE-2013-2566, CVE-2015-2808)
- Ciphers using 64 bit or less are considered to be vulnerable to brute force methods and therefore considered as weak (CVE-2015-4000)
- 1024 bit RSA authentication is considered to be insecure and therefore as weak
- Any cipher considered to be secure for only the next 10 years is considered as medium
- Any other cipher is considered as strong

Vulnerability Detection Method

Checks previous collected cipher suites.

NOTE: No severity for SMTP services with 'Opportunistic TLS' and weak cipher suites on port 25/tcp is reported. If too strong cipher suites are configured for this service the alternative would be to fall back to an even more insecure cleartext communication.

. . . continues on next page . . .

. . . continued from previous page . . .

Details: SSL/TLS: Report Weak Cipher Suites
OID:1.3.6.1.4.1.25623.1.0.103440
Version used: 2025-03-27T05:38:50Z

Product Detection Result
Product: cpe:/a:ietf:transport_layer_security
Method: SSL/TLS: Report Supported Cipher Suites
OID: 1.3.6.1.4.1.25623.1.0.802067)

References

```
cve: CVE-2013-2566
cve: CVE-2015-2808
cve: CVE-2015-4000
url: https://ssl-config.mozilla.org
url: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidel
↪ines/TG02102/BSI-TR-02102-1.html
url: https://www.bsi.bund.de/EN/Themen/Oeffentliche-Verwaltung/Mindeststandards/
↪TLS-Protokoll/TLS-Protokoll_node.html
url: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Technisch
↪eRichtlinien/TR03116/BSI-TR-03116-4.html
url: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Mindeststandards/Mindes
↪tstandard_BSI_TLS_Version_2_4.html
url: https://web.archive.org/web/20240113175943/https://www.bettercrypto.org
url: https://www.enisa.europa.eu/publications/algorithms-key-size-and-parameters
↪-report-2014
cert-bund: CB-K21/0067
cert-bund: CB-K19/0812
cert-bund: CB-K17/1750
cert-bund: CB-K16/1593
cert-bund: CB-K16/1552
cert-bund: CB-K16/1102
cert-bund: CB-K16/0617
cert-bund: CB-K16/0599
cert-bund: CB-K16/0168
cert-bund: CB-K16/0121
cert-bund: CB-K16/0090
cert-bund: CB-K16/0030
cert-bund: CB-K15/1751
cert-bund: CB-K15/1591
cert-bund: CB-K15/1550
cert-bund: CB-K15/1517
cert-bund: CB-K15/1514
cert-bund: CB-K15/1464
cert-bund: CB-K15/1442
cert-bund: CB-K15/1334
cert-bund: CB-K15/1269
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
cert-bund: CB-K15/1136
cert-bund: CB-K15/1090
cert-bund: CB-K15/1059
cert-bund: CB-K15/1022
cert-bund: CB-K15/1015
cert-bund: CB-K15/0986
cert-bund: CB-K15/0964
cert-bund: CB-K15/0962
cert-bund: CB-K15/0932
cert-bund: CB-K15/0927
cert-bund: CB-K15/0926
cert-bund: CB-K15/0907
cert-bund: CB-K15/0901
cert-bund: CB-K15/0896
cert-bund: CB-K15/0889
cert-bund: CB-K15/0877
cert-bund: CB-K15/0850
cert-bund: CB-K15/0849
cert-bund: CB-K15/0834
cert-bund: CB-K15/0827
cert-bund: CB-K15/0802
cert-bund: CB-K15/0764
cert-bund: CB-K15/0733
cert-bund: CB-K15/0667
cert-bund: CB-K14/0935
cert-bund: CB-K13/0942
dfn-cert: DFN-CERT-2023-2939
dfn-cert: DFN-CERT-2021-0775
dfn-cert: DFN-CERT-2020-1561
dfn-cert: DFN-CERT-2020-1276
dfn-cert: DFN-CERT-2017-1821
dfn-cert: DFN-CERT-2016-1692
dfn-cert: DFN-CERT-2016-1648
dfn-cert: DFN-CERT-2016-1168
dfn-cert: DFN-CERT-2016-0665
dfn-cert: DFN-CERT-2016-0642
dfn-cert: DFN-CERT-2016-0184
dfn-cert: DFN-CERT-2016-0135
dfn-cert: DFN-CERT-2016-0101
dfn-cert: DFN-CERT-2016-0035
dfn-cert: DFN-CERT-2015-1853
dfn-cert: DFN-CERT-2015-1679
dfn-cert: DFN-CERT-2015-1632
dfn-cert: DFN-CERT-2015-1608
dfn-cert: DFN-CERT-2015-1542
dfn-cert: DFN-CERT-2015-1518
dfn-cert: DFN-CERT-2015-1406
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
dfn-cert: DFN-CERT-2015-1341
dfn-cert: DFN-CERT-2015-1194
dfn-cert: DFN-CERT-2015-1144
dfn-cert: DFN-CERT-2015-1113
dfn-cert: DFN-CERT-2015-1078
dfn-cert: DFN-CERT-2015-1067
dfn-cert: DFN-CERT-2015-1038
dfn-cert: DFN-CERT-2015-1016
dfn-cert: DFN-CERT-2015-1012
dfn-cert: DFN-CERT-2015-0980
dfn-cert: DFN-CERT-2015-0977
dfn-cert: DFN-CERT-2015-0976
dfn-cert: DFN-CERT-2015-0960
dfn-cert: DFN-CERT-2015-0956
dfn-cert: DFN-CERT-2015-0944
dfn-cert: DFN-CERT-2015-0937
dfn-cert: DFN-CERT-2015-0925
dfn-cert: DFN-CERT-2015-0884
dfn-cert: DFN-CERT-2015-0881
dfn-cert: DFN-CERT-2015-0879
dfn-cert: DFN-CERT-2015-0866
dfn-cert: DFN-CERT-2015-0844
dfn-cert: DFN-CERT-2015-0800
dfn-cert: DFN-CERT-2015-0737
dfn-cert: DFN-CERT-2015-0696
dfn-cert: DFN-CERT-2014-0977
```

[return to 127.0.0.1]

2.2.2 Medium 9392/tcp

Medium (CVSS: 4.3)

NVT: SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection

Product detection result

```
cpe:/a:ietf:transport_layer_security:1.0
Detected by SSL/TLS: Version Detection (OID: 1.3.6.1.4.1.25623.1.0.105782)
```

Summary

It was possible to detect the usage of the deprecated TLSv1.0 and/or TLSv1.1 protocol on this system.

Quality of Detection (QoD): 98%

. . . continues on next page . . .

. . . continued from previous page . . .

Vulnerability Detection Result

```
In addition to TLSv1.2+ the service is also providing the deprecated TLSv1.0 and
↪ TLSv1.1 protocols and supports one or more ciphers. Those supported ciphers c
↪an be found in the 'SSL/TLS: Report Supported Cipher Suites' (OID: 1.3.6.1.4.1
↪.25623.1.0.802067) VT.
```

Impact

An attacker might be able to use the known cryptographic flaws to eavesdrop the connection between clients and the service to get access to sensitive data transferred within the secured connection.

Furthermore newly uncovered vulnerabilities in this protocols won't receive security updates anymore.

Solution:

Solution type: Mitigation

It is recommended to disable the deprecated TLSv1.0 and/or TLSv1.1 protocols in favor of the TLSv1.2+ protocols.

Please see the references for more resources supporting you with this task.

Affected Software/OS

- All services providing an encrypted communication using the TLSv1.0 and/or TLSv1.1 protocols
- CVE-2023-41928: Kiloview P1 4G and P2 4G Video Encoder
- CVE-2024-41270: Gorush v1.18.4
- CVE-2025-3200: Multiple products from Wiesemann & Theis

Vulnerability Insight

The TLSv1.0 and TLSv1.1 protocols contain known cryptographic flaws like:

- CVE-2011-3389: Browser Exploit Against SSL/TLS (BEAST)
- CVE-2015-0204: Factoring Attack on RSA-EXPORT Keys Padding Oracle On Downgraded Legacy Encryption (FREAK)

Vulnerability Detection Method

Checks the used TLS protocols of the services provided by this system.

Details: `SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection`

OID:1.3.6.1.4.1.25623.1.0.117274

Version used: `2025-04-30T05:39:51Z`

Product Detection Result

Product: `cpe:/a:ietf:transport_layer_security:1.0`

Method: `SSL/TLS: Version Detection`

OID: 1.3.6.1.4.1.25623.1.0.105782)

References

`cve: CVE-2011-3389`

. . . continues on next page . . .

. . . continued from previous page . . .

```
cve: CVE-2015-0204
cve: CVE-2023-41928
cve: CVE-2024-41270
cve: CVE-2025-3200
url: https://ssl-config.mozilla.org
url: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidel
↪ines/TG02102/BSI-TR-02102-1.html
url: https://www.bsi.bund.de/EN/Themen/Oeffentliche-Verwaltung/Mindeststandards/
↪TLS-Protokoll/TLS-Protokoll_node.html
url: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Technisch
↪eRichtlinien/TR03116/BSI-TR-03116-4.html
url: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Mindeststandards/Mindes
↪tstandard_BSI_TLS_Version_2_4.html
url: https://web.archive.org/web/20240113175943/https://www.bettercrypto.org
url: https://www.enisa.europa.eu/publications/algorithms-key-size-and-parameters
↪-report-2014
url: https://datatracker.ietf.org/doc/rfc8996/
url: https://vnhacker.blogspot.com/2011/09/beast.html
url: https://web.archive.org/web/20201108095603/https://censys.io/blog/freak
url: https://certvde.com/en/advisories/VDE-2025-031/
url: https://gist.github.com/nyxfqq/cfae38fada582a0f576d154be1aeb1fc
url: https://advisories.ncsc.nl/advisory?id=NCSC-2024-0273
cert-bund: WID-SEC-2023-1435
cert-bund: CB-K18/0799
cert-bund: CB-K16/1289
cert-bund: CB-K16/1096
cert-bund: CB-K15/1751
cert-bund: CB-K15/1266
cert-bund: CB-K15/0850
cert-bund: CB-K15/0764
cert-bund: CB-K15/0720
cert-bund: CB-K15/0548
cert-bund: CB-K15/0526
cert-bund: CB-K15/0509
cert-bund: CB-K15/0493
cert-bund: CB-K15/0384
cert-bund: CB-K15/0365
cert-bund: CB-K15/0364
cert-bund: CB-K15/0302
cert-bund: CB-K15/0192
cert-bund: CB-K15/0079
cert-bund: CB-K15/0016
cert-bund: CB-K14/1342
cert-bund: CB-K14/0231
cert-bund: CB-K13/0845
cert-bund: CB-K13/0796
cert-bund: CB-K13/0790
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
dfn-cert: DFN-CERT-2020-0177
dfn-cert: DFN-CERT-2020-0111
dfn-cert: DFN-CERT-2019-0068
dfn-cert: DFN-CERT-2018-1441
dfn-cert: DFN-CERT-2018-1408
dfn-cert: DFN-CERT-2016-1372
dfn-cert: DFN-CERT-2016-1164
dfn-cert: DFN-CERT-2016-0388
dfn-cert: DFN-CERT-2015-1853
dfn-cert: DFN-CERT-2015-1332
dfn-cert: DFN-CERT-2015-0884
dfn-cert: DFN-CERT-2015-0800
dfn-cert: DFN-CERT-2015-0758
dfn-cert: DFN-CERT-2015-0567
dfn-cert: DFN-CERT-2015-0544
dfn-cert: DFN-CERT-2015-0530
dfn-cert: DFN-CERT-2015-0396
dfn-cert: DFN-CERT-2015-0375
dfn-cert: DFN-CERT-2015-0374
dfn-cert: DFN-CERT-2015-0305
dfn-cert: DFN-CERT-2015-0199
dfn-cert: DFN-CERT-2015-0079
dfn-cert: DFN-CERT-2015-0021
dfn-cert: DFN-CERT-2014-1414
dfn-cert: DFN-CERT-2013-1847
dfn-cert: DFN-CERT-2013-1792
dfn-cert: DFN-CERT-2012-1979
dfn-cert: DFN-CERT-2012-1829
dfn-cert: DFN-CERT-2012-1530
dfn-cert: DFN-CERT-2012-1380
dfn-cert: DFN-CERT-2012-1377
dfn-cert: DFN-CERT-2012-1292
dfn-cert: DFN-CERT-2012-1214
dfn-cert: DFN-CERT-2012-1213
dfn-cert: DFN-CERT-2012-1180
dfn-cert: DFN-CERT-2012-1156
dfn-cert: DFN-CERT-2012-1155
dfn-cert: DFN-CERT-2012-1039
dfn-cert: DFN-CERT-2012-0956
dfn-cert: DFN-CERT-2012-0908
dfn-cert: DFN-CERT-2012-0868
dfn-cert: DFN-CERT-2012-0867
dfn-cert: DFN-CERT-2012-0848
dfn-cert: DFN-CERT-2012-0838
dfn-cert: DFN-CERT-2012-0776
dfn-cert: DFN-CERT-2012-0722
dfn-cert: DFN-CERT-2012-0638
```

. . . continues on next page . . .

... continued from previous page ...

```
dfn-cert: DFN-CERT-2012-0627
dfn-cert: DFN-CERT-2012-0451
dfn-cert: DFN-CERT-2012-0418
dfn-cert: DFN-CERT-2012-0354
dfn-cert: DFN-CERT-2012-0234
dfn-cert: DFN-CERT-2012-0221
dfn-cert: DFN-CERT-2012-0177
dfn-cert: DFN-CERT-2012-0170
dfn-cert: DFN-CERT-2012-0146
dfn-cert: DFN-CERT-2012-0142
dfn-cert: DFN-CERT-2012-0126
dfn-cert: DFN-CERT-2012-0123
dfn-cert: DFN-CERT-2012-0095
dfn-cert: DFN-CERT-2012-0051
dfn-cert: DFN-CERT-2012-0047
dfn-cert: DFN-CERT-2012-0021
dfn-cert: DFN-CERT-2011-1953
dfn-cert: DFN-CERT-2011-1946
dfn-cert: DFN-CERT-2011-1844
dfn-cert: DFN-CERT-2011-1826
dfn-cert: DFN-CERT-2011-1774
dfn-cert: DFN-CERT-2011-1743
dfn-cert: DFN-CERT-2011-1738
dfn-cert: DFN-CERT-2011-1706
dfn-cert: DFN-CERT-2011-1628
dfn-cert: DFN-CERT-2011-1627
dfn-cert: DFN-CERT-2011-1619
dfn-cert: DFN-CERT-2011-1482
```

[return to 127.0.0.1]

2.3 192.168.1.10

Host scan start Wed Jun 25 03:08:12 2025 UTC
Host scan end Wed Jun 25 22:24:04 2025 UTC

Service (Port)	Threat Level
80/tcp	Medium
53/udp	Medium
general/tcp	Low
22/tcp	Low
general/icmp	Low

2.3.1 Medium 80/tcp

Medium (CVSS: 5.0)

NVT: Source Control Management (SCM) Files/Folders Accessible (HTTP)

Summary
The script attempts to identify files/folders of a SCM accessible at the webserver.

Quality of Detection (QoD): 70%

Vulnerability Detection Result

```
The following SCM files/folders were identified:
Match:      0000000000000000000000000000000000000000 461b83ad590e55a0a8af4d51256
↪4d5feb8678c9b root <root@dhcpseerver.(none)> 1750208829 +0000 clone: from http
↪s://github.com/digininja/DVWA.git
Used regex: ^[a-f0-9]{40} [a-f0-9]{40}
URL:        http://192.168.1.10/DVWA/.git/logs/HEAD
Match:      [core]
[remote "origin"]
[branch "master"]
Used regex: ^\[(core|receive|(remote|branch) .+)\]$
URL:        http://192.168.1.10/DVWA/.git/config
Match:      # git ls-files --others --exclude-from=.git/info/exclude
Used regex: ^# git ls-files
URL:        http://192.168.1.10/DVWA/.git/info/exclude
Match:      DIRC
Used regex: ^DIRC
URL:        http://192.168.1.10/DVWA/.git/index
Match:      Unnamed repository; edit this file 'description' to name the reposit
↪ory.
Used regex: ^Unnamed repository
URL:        http://192.168.1.10/DVWA/.git/description
Match:      ref: refs/heads/master
Used regex: ^ref: refs/
URL:        http://192.168.1.10/DVWA/.git/HEAD
```

Impact
Based on the information provided in these files/folders an attacker might be able to gather additional info about the structure of the system and its applications.

Solution:
Solution type: Mitigation
Restrict access to the SCM files/folders for authorized systems only.

Vulnerability Insight
Currently the script is checking for files/folders of the following SCM software:
- Git (.git)

. . . continues on next page . . .

. . . continued from previous page . . .

- Mercurial (.hg)
- Bazaar (.bzr)
- CVS (CVS/Root, CVS/Entries)
- Subversion (.svn)

Vulnerability Detection Method
Check the response if SCM files/folders are accessible.
Details: `Source Control Management (SCM) Files/Folders Accessible (HTTP)`
OID:1.3.6.1.4.1.25623.1.0.111084
Version used: `2023-08-01T13:29:10Z`

References

```
url: http://pen-testing.sans.org/blog/pen-testing/2012/12/06/all-your-svn-are-be
↪long-to-us
url: https://github.com/anantshri/svn-extractor
url: https://blog.skullsecurity.org/2012/using-git-clone-to-get-pwn3d
url: https://blog.netspi.com/dumping-git-data-from-misconfigured-web-servers/
url: http://resources.infosecinstitute.com/hacking-svn-git-and-mercurial/
```

Medium (CVSS: 4.8)

NVT: Cleartext Transmission of Sensitive Information via HTTP

Summary
The host / application transmits sensitive information (username, passwords) in cleartext via HTTP.

Quality of Detection (QoD): 80%

Vulnerability Detection Result

```
The following input fields were identified (URL:input name):
http://192.168.1.10/DVWA/login.php:password
```

Impact
An attacker could use this situation to compromise or eavesdrop on the HTTP communication between the client and the server using a man-in-the-middle attack to get access to sensitive data like usernames or passwords.

Solution:
Solution type: Workaround
Enforce the transmission of sensitive data via an encrypted SSL/TLS connection. Additionally make sure the host / application is redirecting all users to the secured SSL/TLS connection before allowing to input sensitive data into the mentioned functions.

Affected Software/OS

. . . continues on next page . . .

. . . continued from previous page . . .

Hosts / applications which doesn't enforce the transmission of sensitive data via an encrypted SSL/TLS connection.

Vulnerability Detection Method
Evaluate previous collected information and check if the host / application is not enforcing the transmission of sensitive data via an encrypted SSL/TLS connection.
The script is currently checking the following:
- HTTP Basic Authentication (Basic Auth)
- HTTP Forms (e.g. Login) with input field of type 'password'
Details: `Cleartext Transmission of Sensitive Information via HTTP`
OID:1.3.6.1.4.1.25623.1.0.108440
Version used: `2023-09-07T05:05:21Z`

References

```
url: https://www.owasp.org/index.php/Top_10_2013-A2-Broken_Authentication_and_Se
↪ssion_Management
url: https://www.owasp.org/index.php/Top_10_2013-A6-Sensitive_Data_Exposure
url: https://cwe.mitre.org/data/definitions/319.html
```

[return to 192.168.1.10]

2.3.2 Medium 53/udp

Medium (CVSS: 5.0)

NVT: DNS Cache Snooping Vulnerability (UDP) - Active Check

Summary
The DNS server is prone to a cache snooping vulnerability.

Quality of Detection (QoD): 70%

Vulnerability Detection Result

```
Received (an) answer(s) for a non-recursive query for "example.com".
Result:
23.215.0.138
```

Impact
Attackers might gain information about cached DNS records which might lead to further attacks.
Note: This finding might be an acceptable risk if you:
- trust all clients which can reach the server
- do not allow recursive queries from outside your trusted client network.

Solution:
Solution type: Mitigation

. . . continues on next page . . .

. . . continued from previous page . . .

There are multiple possible mitigation steps depending on location and functionality needed by the DNS server:
- Disable recursion
- Don't allow public access to DNS Servers doing recursion
- Leave recursion enabled if the DNS Server stays on a corporate network that cannot be reached by untrusted clients
- If the risk is accepted either create an override for this result or configure the 'Private LAN' setting mentioned earlier

Vulnerability Insight

DNS cache snooping is when someone queries a DNS server in order to find out (snoop) if the DNS server has a specific DNS record cached, and thereby deduce if the DNS server's owner (or its users) have recently visited a specific site.
This may reveal information about the DNS server's owner, such as what vendor, bank, service provider, etc. they use. Especially if this is confirmed (snooped) multiple times over a period.
This method could even be used to gather statistical information - for example at what time does the DNS server's owner typically access his net bank etc. The cached DNS record's remaining TTL value can provide very accurate data for this.
DNS cache snooping is possible even if the DNS server is not configured to resolve recursively for 3rd parties, as long as it provides records from the cache also to 3rd parties (a.k.a. 'lame requests').

Vulnerability Detection Method

Sends a crafted DNS query and checks the response.
Notes:
- No scan result is expected if localhost (127.0.0.1) was scanned (self scanning)
- If the scanned network is e.g. a private LAN which contains systems not accessible to the public (access restricted) and it is accepted that the target host is disclosing information to this network please set the 'Network type' configuration of the following VT to 'Private LAN':
Global variable settings (OID: 1.3.6.1.4.1.25623.1.0.12288)
Details: `DNS Cache Snooping Vulnerability (UDP) - Active Check`
OID:1.3.6.1.4.1.25623.1.0.146591
Version used: `2025-05-01T05:40:03Z`

References

```
url: https://www.cs.unc.edu/~fabian/course_papers/cache_snooping.pdf
url: https://docs.microsoft.com/en-us/troubleshoot/windows-server/networking/dns
↪-server-cache-snooping-attacks
url: https://kb.isc.org/docs/aa-00509
url: https://kb.isc.org/docs/aa-00482
```

[return to 192.168.1.10]

2.3.3 Low general/tcp

Low (CVSS: 2.6)

NVT: TCP Timestamps Information Disclosure

Summary
The remote host implements TCP timestamps and therefore allows to compute the uptime.

Quality of Detection (QoD): 80%

Vulnerability Detection Result

```
It was detected that the host implements RFC1323/RFC7323.
The following timestamps were retrieved with a delay of 1 seconds in-between:
Packet 1: 91516610
Packet 2: 91517666
```

Impact
A side effect of this feature is that the uptime of the remote host can sometimes be computed.

Solution:
Solution type: Mitigation
To disable TCP timestamps on linux add the line 'net.ipv4.tcp_timestamps = 0' to /etc/sysctl.conf. Execute 'sysctl -p' to apply the settings at runtime.
To disable TCP timestamps on Windows execute 'netsh int tcp set global timestamps=disabled'
Starting with Windows Server 2008 and Vista, the timestamp can not be completely disabled.
The default behavior of the TCP/IP stack on this Systems is to not use the Timestamp options when initiating TCP connections, but use them if the TCP peer that is initiating communication includes them in their synchronize (SYN) segment.
See the references for more information.

Affected Software/OS
TCP implementations that implement RFC1323/RFC7323.

Vulnerability Insight
The remote host implements TCP timestamps, as defined by RFC1323/RFC7323.

Vulnerability Detection Method
Special IP packets are forged and sent with a little delay in between to the target IP. The responses are searched for a timestamps. If found, the timestamps are reported.
Details: `TCP Timestamps Information Disclosure`
OID:1.3.6.1.4.1.25623.1.0.80091
Version used: `2023-12-15T16:10:08Z`

References

```
url: https://datatracker.ietf.org/doc/html/rfc1323
url: https://datatracker.ietf.org/doc/html/rfc7323
url: https://web.archive.org/web/20151213072445/http://www.microsoft.com/en-us/d
```

. . . continues on next page . . .

. . . continued from previous page . . .

```
↪ownload/details.aspx?id=9152
url: https://www.fortiguard.com/psirt/FG-IR-16-090
```

[return to 192.168.1.10]

2.3.4 Low 22/tcp

Low (CVSS: 2.6)

NVT: Weak MAC Algorithm(s) Supported (SSH)

Product detection result

```
cpe:/a:ietf:secure_shell_protocol
Detected by SSH Protocol Algorithms Supported (OID: 1.3.6.1.4.1.25623.1.0.105565
↪)
```

Summary

The remote SSH server is configured to allow / support weak MAC algorithm(s).

Quality of Detection (QoD): 80%

Vulnerability Detection Result

```
The remote SSH server supports the following weak client-to-server MAC algorithm
↪(s):
umac-64-etm@openssh.com
umac-64@openssh.com
The remote SSH server supports the following weak server-to-client MAC algorithm
↪(s):
umac-64-etm@openssh.com
umac-64@openssh.com
```

Solution:

Solution type: Mitigation

Disable the reported weak MAC algorithm(s).

Vulnerability Detection Method

Checks the supported MAC algorithms (client-to-server and server-to-client) of the remote SSH server.

Currently weak MAC algorithms are defined as the following:

- MD5 based algorithms
- 96-bit based algorithms
- 64-bit based algorithms
- 'none' algorithm

. . . continues on next page . . .

. . . continued from previous page . . .

Details: `Weak MAC Algorithm(s) Supported (SSH)`
OID:1.3.6.1.4.1.25623.1.0.105610
Version used: `2024-06-14T05:05:48Z`

Product Detection Result
Product: `cpe:/a:ietf:secure_shell_protocol`
Method: `SSH Protocol Algorithms Supported`
OID: 1.3.6.1.4.1.25623.1.0.105565)

References
```
url: https://www.rfc-editor.org/rfc/rfc6668
url: https://www.rfc-editor.org/rfc/rfc4253#section-6.4
```

[return to 192.168.1.10]

2.3.5 Low general/icmp

Low (CVSS: 2.1)

NVT: ICMP Timestamp Reply Information Disclosure

Summary
The remote host responded to an ICMP timestamp request.

Quality of Detection (QoD): 80%

Vulnerability Detection Result
```
The following response / ICMP packet has been received:
- ICMP Type: 14
- ICMP Code: 0
```

Impact
This information could theoretically be used to exploit weak time-based random number generators in other services.

Solution:
Solution type: Mitigation
Various mitigations are possible:
- Disable the support for ICMP timestamp on the remote host completely
- Protect the remote host by a firewall, and block ICMP packets passing through the firewall in either direction (either completely or only for untrusted networks)

Vulnerability Insight

. . . continues on next page . . .

. . . continued from previous page . . .

The Timestamp Reply is an ICMP message which replies to a Timestamp message. It consists of the originating timestamp sent by the sender of the Timestamp as well as a receive timestamp and a transmit timestamp.

Vulnerability Detection Method

Sends an ICMP Timestamp (Type 13) request and checks if a Timestamp Reply (Type 14) is received.

Details: `ICMP Timestamp Reply Information Disclosure`

OID:1.3.6.1.4.1.25623.1.0.103190

Version used: `2025-01-21T05:37:33Z`

References

```
cve: CVE-1999-0524
url: https://datatracker.ietf.org/doc/html/rfc792
url: https://datatracker.ietf.org/doc/html/rfc2780
cert-bund: CB-K15/1514
cert-bund: CB-K14/0632
dfn-cert: DFN-CERT-2014-0658
```

[return to 192.168.1.10]

This file was automatically generated.